Remarks

Claims 1, 2, 3, 5, 7 through 25, 27 and 29 through 43 and 45 through 61 remain pending in the application. Claims 38 and 49 are amended and claims 44 is cancelled.

Claims 38 and 49 are amended to incorporate the feature of dependent claim 44, defining that the operation to be executed is a fingerprint-matching algorithm comprising a base minutiae finding process and a minutiae matching process. The amendments further define that the base minutiae finding process and the minutiae matching process are respectively a first stage and a second stage of a biometric identity authentication process, and to further include the features of an open portion of a biometric identification template used in said biometric identity authentication as correspondingly defined in claim 1. Support for this amendment can be found from page 34, last paragraph to page 36, second last paragraph of the specification, from which it could be derived that the fingerprint matching algorithm described earlier (i.e. in accordance with claim 1) can be performed using the method of distributed computing on first and second processors in accordance with amended claims 38 and 49.

Claims 1, 2, 3, 5, 7 through 25, 27 and 29 through 61 stand rejected under 35 U.S.C. § 102(b) as anticipated by Hamid, Method and Apparatus for Hashing Data, U.S. Patent 7,274,804 (Sep. 25, 2007).

The Examiner asserts that Hamid discloses a method wherein a biometric identification template is divided into a secure portion (e.g. private portion) and an open portion (e.g. public

portion). The public portion in paragraphs 26-27 of Hamid is considered to be an open portion, which is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template.

It is noticed that said public portion in paragraphs 26-27 of Hamid is a portion of the biometric template, which surrenders information corresponding to a portion of biometric sample. As described in paragraph 28 of Hamid, when this public portion is received by a client terminal (e.g. host processor), a third party with access to the client terminal obtains sufficient information to reconstruct within statistical limits portions of an image of the fingerprint. The reconstructed portions of the image of the fingerprint can be modified by an imposter to cause an impostor to be incorrectly authenticated as a genuine user. Therefore, the public portion in paragraphs 26-27 of Hamid contains data unauthorized modification of which may cause an impostor to be incorrectly authenticated as a genuine user, in contrast to the open portion claimed in claim 1 of the present application which contains data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user.

In addition, paragraph 34 of Hamid discloses a public portion which is hashed data in the form of offset locations relative to feature locations associated with the biometric template, wherein the plurality of offset locations is a known offset from identifiable features. Paragraph 34 of Hamid further discloses that the hash function used to hash the template data results in a repeatable offset, or need to be synchronized

between the smart card and the host, or need to be provided from the smart card to the host. This would leak the information of the hash function to the host. Thus, the host (i.e. the client terminal) of Hamid has knowledge of the offset and the hash function, and would be able to reconstruct the locations of the features in the biometric template using the knowledge of the offset and the hash function. For example, if the hash function F1 in paragraph 48 and the offset s, t of the function F1 are known to the host, an imposter with access to the host may recover original template data, e.g. the minutia location, from the hashed template data. An imposter may also be able to estimate the minutia direction using the information of the transformed template data and the known offset s, t of the hash function F1. Thus, the imposter may modify the recovered/estimated template data, which when sent back to the smart card for correlation may cause the impostor to be incorrectly authenticated as a genuine user.

Accordingly, the public portion in paragraph 34 of Hamid surrenders the information of the biometric template, and can be modified by a hacker to produce modified data relating to a plurality of features which is sent to the smart card for correlation (as in paragraph 36 of Hamid). Thus, the public portion in paragraph 34 of Hamid also contains data unauthorized modification of which may cause an impostor to be incorrectly authenticated as a genuine user, in contrast to the open portion claimed in claim 1 of the present application which contains data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user.

In view of the above, Hamid does not disclose an open portion of a biometric identification template as defined in claim 1 of the present application. The open portion as in claim 1 of the present application is transmitted out of the user-presented device to the client terminal for use in a first stage of a biometric identity authentication process, and would not be modified by an imposter to construct a fake biometric identification template. Rather, the public portion as disclosed in Hamid surrenders the information of the biometric template, and can be used by an imposter to produce fake data for correlation. Thus, the method of claim 1 is not anticipated by Hamid and the rejection with respect to claim 1 should be withdrawn

Claims 3, 5, and 7 through 23 depend from claim 1 and thus are not anticipated by Hamid.

For the similar reasons, the system of claim 24 corresponding to the method of claim 1 is not anticipated by Hamid. The subject matter of dependent claims 25, 27 and 29-37 is accordingly not anticipated by Hamid.

Claim 2 defines a method of registration of a user according to a biometric parameter of the user, wherein a computed biometric identification template is divided into secure portion and open portion at the authorized client terminal. The open portion contains data unauthorized modification of which may not cause an imposter to be incorrectly authenticated as a genuine user.

As discussed above, Hamid does not disclose dividing a biometric template into a secure portion and an open portion, wherein the open portion contains data unauthorized modification

of which may not cause an imposter to be incorrectly authenticated as a genuine user.

Therefore, the subject matter of claim 2 is not anticipated by Hamid.

Claims 38 through 43 and 45 through 61 are also rejected under 35 USC 102(e) as being anticipated by Studd, Method and System for Executing Applications on a Mobile Device, U.S. Patent Application Publication 2004/0122774 (Jun. 24, 2004).

Applicant respectfully submits that the claimed subject matter of amended claims 38 is not anticipated by Studd.

Claim 38 is amended to define that the operation to be executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor. In addition, claim 38 is amended to define that the base minutiae finding process and the minutiae matching process are respectively a first stage and a second stage of a biometric identity authentication process, and to further include the features of an open portion of a biometric identification template used in said biometric identity authentication.

Studd does not disclose a method of executing an operation, wherein the operation is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor.

In addition, the Examiner points out in No. 29 of the Office Action that Studd teaches a request for a list of mobile

service applications from mobile to device, corresponding to the feature of storing in the first processor a first task table containing a plurality of process names with associated processor identifiers in claim 38 of the present application. However, the method of Studd requests for a list of applications from a mobile, which makes the mobile leak the list outside. In contrast, the method of claim 38 stores, i.e. pre-stores, a first task table in the first processor, and does not request for such a task table from a second processor. Thus, the method of claim 38 is secure that a task table in the second processor is not disclosed to the outside during the execution of the method.

In view of the above, Studd does not disclose the method claimed in claim 38. Therefore, the subject matter of claim 38 and of its dependent claims 39-43, 45-48 is not anticipated by Studd.

For the reasons analogous to the above, the system of claim 49 corresponding to the method of claim 38 is not anticipated by Studd, either. Accordingly, the subject matter of the dependent claims 50-61 is new over Studd.

For the reasons set forth above, applicant respectfully submits that present claims 1, 2, 3, 5, 7 through 25, 27 and 29 through 43 and 45 through 61 are patentable under 35 U.S.C. §102.

The Examiner also asserted in No. 53 of the Office Action that Hamid discloses a method, wherein the operation being executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor.

However, as discussed above, Hamid does not disclose or suggest a method wherein the open portion of a biometric identification template contains data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user.

In view of the above, the proposed combination of Studd and Hamid discloses or suggests the features as defined in amended claim 38 of the present application. Therefore, the subject matter of claim 38 and of its dependent claims 39-43, 45-48 is not obvious from the combination of Studd and Hamid.

For the reasons analogous to the above, the system of claim 49-61 corresponding to the method of claim 38 is also not rendered obvious by the proposed combination of Studd and Hamid.

Claim 44 stands rejected under 35 U.S.C §103(a) as unpatentable over Studd in view of Hamid. Claim 44 is cancelled and thus this rejection is moot.

Conclusion

This response has addressed all of the Examiner's grounds for rejection. The rejections based on prior art have been traversed. Reconsideration of the rejections and allowance of the claims is requested.

Date: May 18, 2009

By: /Paul J. Backofen/
Paul J. Backofen, Esq.
Reg. No. 42278